

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

PROSKAUER ROSE LLP,
Plaintiff,

Case No. _____

- against -

JONATHAN O'BRIEN,
Defendant.

DECLARATION OF YONG C. HSU IN SUPPORT OF PLAINTIFF'S MOTION FOR *EX PARTE* TEMPORARY RESTRAINING ORDER

I, Yong ("Ken") C. Hsu, hereby declare as follows,

1. I am the Information Security and Technology Officer at plaintiff Proskauer Rose LLP ("Proskauer" or the "Firm"), an international law firm based in New York City. I have personal knowledge of the facts set forth herein and, if called to do so, could competently testify thereto.

2. I have worked at Proskauer Rose since 2012 and have served in my current role since 2019. I report to the Firm's Chief Information Officer, who reports to the Firm's Chief Operating Officer, defendant Jonathan O'Brien ("Mr. O'Brien").

3. In my role, I have two primary responsibilities. First, I oversee the Firm's engineering and technology efforts. Second, I oversee the Firm's security, privacy, and risk management efforts to safeguard the Firm's confidential and sensitive information.

4. During my time at the Firm, Proskauer's information security and data privacy efforts have earned the Firm two prestigious certifications from the International Organization for Standardization ("ISO"). In 2015, Proskauer became one of the first law firms to receive the ISO

27001 certification. ISO 27001 provides an international methodology for the implementation, management, and maintenance of information security. The Firm maintains this certification through independent yearly internal and external audits that test the security of our systems. Proskauer is currently ISO certified in eight areas of information security where client and personal data may be stored or transferred, including: document management system, data backup, mobile device management, remote access, email service, client collaboration service, client relationship management service, and active directory management service.

5. In 2021, Proskauer became one of the few law firms to receive the ISO 27701 certification, which provides specific requirements for establishing, implementing, maintaining, and continually improving our data privacy systems. The Firm takes its clients' data seriously and continues to update its systems to remain compliant with ISO standards and applicable data protection, privacy laws, and regulations.

Proskauer's Data Protection and Information Security Efforts

6. Because of the highly confidential, sensitive, and valuable nature of the information that Proskauer maintains, maintaining the security of the Firm's systems is critical. Accordingly, the Firm's Information Services team, of which I am a member, employs approximately eight people dedicated to achieving the Firm's security objectives. These objectives include implementing and maintaining a robust system of controls, policies, and procedures in light of best practices, industry guidance, and the ever-evolving sophistication in the cyber security threat landscape. In addition, the Information Security team provides detailed security training to all new hires and ongoing training to existing employees.

7. All users of Firm technology resources are uniquely identified and authenticated before being granted access to Firm information. Those resources include, without limitation,

desktops, laptop computers, and mobile devices, including iPhones and iPads. Firm passwords have a required complexity and must be changed on a periodic basis. When employees remotely access the Firm's network and files outside the office, the user IDs and passwords are augmented with an additional, second factor authentication to further authenticate the identity of the user accessing the system.

8. Firm employees are provided with Firm-issued workstations (either desktops or laptops), and my team monitors the status and usage of those workstations on an ongoing basis. Since 2020, Mr. O'Brien has utilized four workstations: (i) a Firm desktop in his New York office, (ii) a Firm laptop in his Manhattan apartment, (iii) a Firm laptop in his home in upstate New York, and (iv) an additional Microsoft Surface laptop that the Firm was testing for potential use by its employees.

9. Proskauer implements detailed policies and technical controls to try to ensure that electronic communication with clients and any other third parties with regard to the Firm's business and client matters are transmitted only through the Firm's technology resources. Firm computers and laptops must run Firm-approved antivirus software and any other protective software the Firm designates to protect against viruses, worms, Trojan horses, spyware, malware, key logging software, and other harmful code.

10. To further protect Proskauer's confidential information, the Firm's technology resources are continually monitored. Intrusion Detection Systems (IDS) are used to provide 24/7 monitoring and audit records of unauthorized attempts to access the technology resources, as well as login failures, use of privileged accounts, changes to access modules or file permissions, modification to installed software or the operating system, and changes to user permissions or privileges. Security logs are maintained for at least twelve (12) months. Access to security logs

is restricted to only authorized personnel from the Firm's Information Security and Engineering Department.

11. While employees must satisfy the authentication requirements I described above to even connect to the Firm's systems, doing so does not grant them access to all Firm data. Instead, the Firm has implemented a system of restrictions to control and monitor employees' access and information rights.

12. Firm data are primarily stored across three main platforms, all residing in the Firm's network: (1) Filesite, (2) the R Drive, and (3) Sharepoint.

- a. Filesite. Filesite is a document management system. It is an "open" system, which means access is generally not restricted unless a client asks for restrictions or users take steps to restrict access to individual files or folders.
- b. R Drive. The "R Drive" is a shared, network drive used by many of the Firm's departments, including business services teams such as Finance and Human Resources. It is a restricted environment in which access to any particular folder must be affirmatively granted to a specific, authorized and authenticated user. Because employees do not have access to materials on this drive absent such a grant, the folders and files are generally not password protected. Nevertheless, it is my understanding that some materials on the R Drive are password protected due to the sensitive nature of the information.
- c. Sharepoint. Sharepoint is a system the Firm uses to host internal "portals," which are used as another way for different departments and groups within the Firm to share information across specific authorized and authenticated users. Like the R Drive, employees do not have access unless it has been specifically granted to them,

and some materials within Sharepoint may also have additional access restrictions such as password protection or restrictions on downloading, saving, or printing.

13. By virtue of his role as the Firm's COO, Mr. O'Brien had the requisite permissions to access the most sensitive of these repositories. In the ordinary course, Mr. O'Brien has also saved and accessed documents on his desktop, which, for backup purposes, is continuously replicated to the Firm's "H Drive," another network drive that is personal to each individual user.

14. In addition to these technological access restrictions, Firm employees are also obligated to follow the Firm's policies regarding computer use when employees join the Firm and, thereafter, on an annual basis. I am personally responsible for the implementation and acknowledgements relating to the Firm's "Computer and Communications Use and Data Protection Policy."

15. That policy was last distributed to employees on December 13, 2022. Six days earlier, on December 7, 2022, I emailed Mr. O'Brien a draft of the updates to the prior year's policy and informed him that there were no material changes. He told me that he was "fine" with the draft. A true and correct copy of those emails are attached hereto as Exhibit 1. After the policy was distributed to Firm employees, Mr. O'Brien acknowledged that he had reviewed this policy, and agreed to comply with it, on December 14, 2022.

16. The policy details the Firm's safeguards to protect Firm, client, lawyer, and employee data. Section 9.1 states, in relevant part, that the Firm's Confidential Information, including information related to "the internal business of the Firm," should "not be accessed in the absence of a legitimate business need or Firm objective." It also states that Confidential Information (i) should not be disclosed to third parties, (ii) "should be kept within the Firm's secured Technology Resources, or its secured office premises, or its authorized offsite storage

facilities,” and (iii) “should not be transmitted via the Internet or wireless network” or “stored on a mobile device or removable media without encrypting Highly Sensitive Information using Firm-approved encryption software and protocols.”

17. Under Section 8.3, Confidential Information includes, among other things, (i) “Firm trade secrets, methodologies, business strategies, business plans, information about clients, and other competitor-sensitive information,” (ii) Firm personnel and client lists, (iii) Firm development programs and unpublished marketing materials, (iv) Firm financial, operational, and accounting information, (v) other nonpublic information relating to the business operations of the Firm, and (vi) data that the Firm is obligated to keep confidential pursuant to an agreement.

18. Consistent with these policies, since 2015, the Firm has implemented technological controls on Firm-issued computers to prohibit the copying of data to “removable media,” such as USB thumb drives. (Such copying is not possible with non-Firm-issued computers.) The Firm grants exceptions to those restrictions only for legitimate business reasons. To request an exception, employees must submit a service request within the Firm’s service management system and explain, among other things, the business reason for the request. While senior lawyers and employees commonly contact the Firm’s IT personnel directly and ask them to submit service requests on their behalf, all requests proceed through that same system.

19. Specific exception requests, along with the stated business reasons for them, are logged and kept for security purposes in the ordinary course of Firm operations. From my review of the records the Firm keeps in the ordinary course of its operations, there is no record of Mr. O’Brien ever requesting access to download files to removable media prior to December 2022.

20. Further, to preserve data relating to actual or threatened litigation against the Firm, the Firm also has procedures related to “litigation holds,” a prophylactic step to deactivate the

Firm's ordinary document retention policies. Under the Firm's ordinary document retention policies, emails older than one year are generally deleted from the user's Outlook mailbox unless the user takes steps to archive them. But under a litigation hold, employees do not have the capability to delete any emails or other information from their mailboxes for the duration of the hold period. Once the hold is lifted, all emails older than one year are instantly deleted from the user's Outlook mailbox.

21. While my team is responsible for the technological steps of activating and deactivating litigation holds, we do so only at the direction of the Firm's General Counsel's office or its identified designees.

Detection of Mr. O'Brien's Theft

22. In the afternoon on Tuesday, December 20, 2022, I received a call from my supervisor, who told me that Mr. O'Brien had resigned and asked me to initiate the Firm's routine monitoring processes for departing employees. Under those processes, whenever an employee resigns, my team conducts a thirty-day activity report to identify any suspicious activity over the preceding thirty days. We also refresh that report each Friday and implement other technical controls to prevent departing employees from sending emails to their personal email addresses.

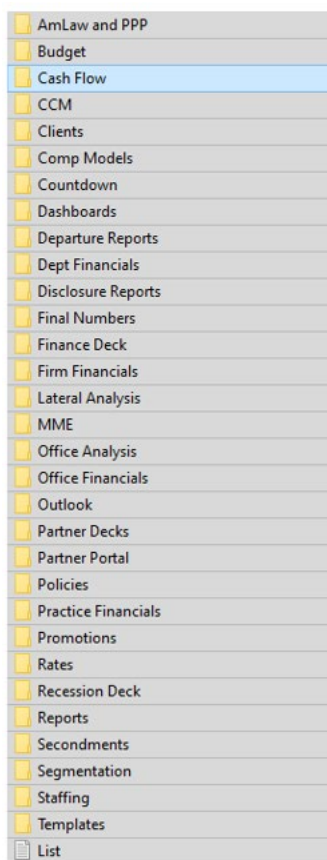
23. My team ran that report for Mr. O'Brien at approximately 2:48 pm on December 20, 2022. At 6:01 pm, I emailed the Firm's Managing Partner and General Counsel with the results. Because the report confirmed that Mr. O'Brien had downloaded files to a USB drive the Managing Partner and General Counsel directed me and my team to launch a forensic investigation, which revealed that Mr. O'Brien had taken a series of actions to steal the Firm's proprietary information and data.

24. From reviewing records of Mr. O'Brien's computer usage for the past 30 days, and archived copies of materials he created, my team and I have been able to reconstruct certain of the actions he took during that time. On Tuesday, November 29, 2022, Mr. O'Brien used his Firm computer to create a Personal Storage Table ("PST") file, "Saved.PST," on his desktop. A PST file is used to store copies of messages, calendar events, and other items within an email server. But because Mr. O'Brien's desktop is automatically replicated in the H-Drive, I was able to see that Mr. O'Brien populated that file with approximately 34 gigabytes of emails and attachments from his Proskauer Outlook mailbox. At the time, Mr. O'Brien had over 100 gigabytes in his Outlook mailbox.

25. On December 5, 2022, at approximately 4:08 pm, Mr. O'Brien copied "Saved.PST" from his Firm-issued computer to a Kingston USB thumb drive. While Mr. O'Brien's Firm-issued computers had been subject to the Firm's restrictions on using removable media, my review of the Firm's service management system revealed that Mr. O'Brien obtained a policy exception earlier that day.

26. Less than an hour later, at approximately 5:06 pm, Mr. O'Brien e-mailed one of the firm's eDiscovery consultants and asked her to release him from a litigation hold that had been in place since 2020. The eDiscovery consultant reminded Mr. O'Brien that emails older than one year would be deleted once the hold was lifted and asked him if he stored everything he needed. Mr. O'Brien told the eDiscovery consultant that he did and that he was on a "clean up mission." A true and correct copy of those emails, which I personally retrieved from the Firm's systems are attached hereto collectively as Exhibit 2. The litigation hold was later lifted, and everything over a year old—approximately 66 gigabytes of emails and attachments—was deleted. At that point, Mr. O'Brien also manually deleted more than 2,000 emails from his Outlook mailbox.

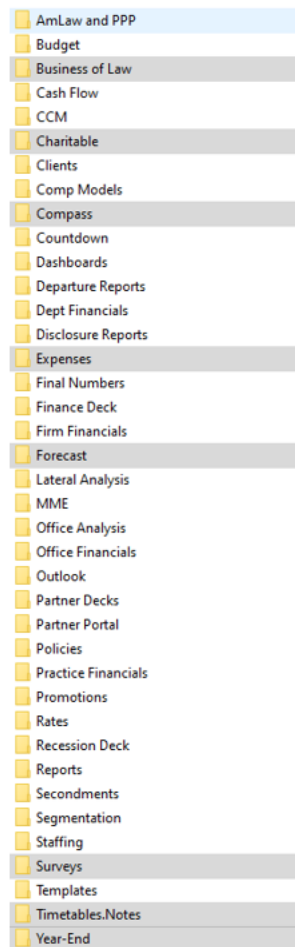
27. Approximately two hours later, at 7:08 pm, Mr. O'Brien copied more than 100 additional files to the same thumb drive, totaling nearly 200 megabytes. Proskauer's technological controls automatically logged the names of every file that Mr. O'Brien copied to the thumb drive. In connection with reviewing Mr. O'Brien's suspicious activity, employees at my direction searched for these files on an archived copy of Mr. O'Brien's computer. They ultimately located them in a folder entitled "MP," which was further organized into thirty-one topical folders, depicted here:



28. The files in that folder roughly corresponded to, and included, a "List.txt" that Mr. O'Brien had saved to his Firm computer weeks earlier, on November 14, 2022.

29. On the morning of December 16, at approximately 10:44 am, Mr. O'Brien and one of his subordinates appear to have created a compressed ".zip" file containing 1,138 files, totaling

1.45 gigabytes of data. This file was ultimately named, “2022 tax documents.zip” and, at 1:07 pm, Mr. O’Brien copied it to a second USB thumb drive, a Verbatim “Store-N-Go.” It contained the 31 folders with the same names as the sub-folders in the “MP” folder,” and eight additional folders, highlighted below in gray below:



30. Of the 1,138 files in “2022 tax documents.zip,” 833 of them were located in a folder called “Compass.” A number of these 833 files are database scripts, with a “.sql” extension, which allow the user to pull data and create reports. Such files are typically reusable with modification. The Firm spends a lot of time developing these scripts across different teams, and copying them would save considerable time compared to creating new ones from scratch.

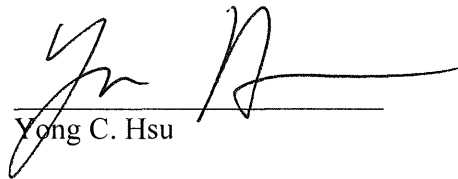
31. The other thirty-one folders also contained documents that were not in the first set that Mr. O'Brien stole on December 5. For example, the "Dashboards" folder contains information relating to newly-created, proprietary software tools (which we refer to as "Dashboards") developed in 2022 and, in some cases, not yet fully completed or made available to Firm partners. These Dashboards were developed over many months by Firm personnel in our Finance group, using significant know-how and resources. They are tools unique to the Firm's business and are valuable management tools. The Dashboard file Mr. O'Brien stole contains folders entitled "Backup Codes", "Data Model", "Executive Dashboard User Guide", "Lawyer Performance Dashboard", "Lawyer Performance Dashboard Outstanding Items," and "Power BI Executive Dashboard", which appears to be a Microsoft file for the code used to create one or more of the Dashboards. He stole software code, data models, user guides, the Microsoft creation tool, and a list of outstanding items for the Dashboard under development.

32. Minutes later, starting at approximately 1:21 pm on December 16, Mr. O'Brien manually deleted the entirety of his H drive, including all 1,138 of the files he copied to the USB drive, and 1,773 other files. He then immediately emptied his "recycling bin," where all of those deleted files otherwise would have been stored.

33. On December 24, 2022, I searched Mr. O'Brien's Firm office, but I was not able to locate either of the two thumb drives. In addition, while I understand that Mr. O'Brien has been on vacation since December 22, I have been monitoring his email. Those monitoring efforts confirmed that Mr. O'Brien was still using his Firm email address (jobrien@proskauer.com) during his vacation and had forwarded various emails from that email address to his personal email address—jonathan_obrien@msn.com—including as recently as December 21, 2022.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing statements are true and correct to the best of my knowledge.

Dated: New York, New York
December 27, 2022



Yong C. Hsu